Auditing for Privacy

CHRISTINE EASTER*

ABSTRACT

In the new digital age, an increase in information sharing and identity theft has sparked concerns with respect to privacy. In order to enhance security and confidence in information sharing systems, the federal government has created many auditing regimes to ensure privacy. This paper examines two types of privacy auditing regimes: those that place privacy auditing requirements on the private sector and those that require oversight of federal agencies. The primary privacy auditing regimes for the private sector include Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act, and Sarbanes-Oxley, while three of the vehicles for oversight of federal agencies are Government Information Security Reform Act/Federal Information Security Management Act, Chief Privacy Officers, and the U.S. Government Accountability Office. This paper analyzes each of these privacy auditing regimes and compares them in terms of their robustness, specificity, and scalability. Finally, this paper considers the use of immutable audit logs as a mechanism for increasing security and ensuring compliance with these various auditing regimes.

I. INTRODUCTION

Not surprisingly, privacy has become a major concern amongst Americans over the past decade. In an era where a vast amount of information is stored electronically, the personal and financial data of consumers and the confidential and secure data of the U.S. government are more susceptible than ever to unauthorized access and corruption. In response to the increasing concerns about privacy, the federal government has passed a number of laws related to privacy over the past ten years. These privacy auditing regimes may be placed into two distinct categories: those that place privacy auditing requirements on the private sector and those that require oversight of federal agencies. Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act, and Sarbanes-Oxley are amongst the primary privacy auditing regimes for the private sector, while Government Information Security Reform Act/Federal Information Security

* Christine Easter is a candidate for juris doctor at The Ohio State University Moritz College of Law, class of 2007. Christine has a B.S. in marketing and decision science from Miami University of Ohio and a M.B.A. with a focus in management information systems and technology enabled business from the University of Dayton.

Management Act, Chief Privacy Officers, and the U.S. Government Accountability Office are amongst the vehicles for oversight of the federal government. These various auditing regimes vary greatly in regards to their robustness, specificity, and scalability. Although some of these regimes, particularly the private sector regimes, do not explicitly require the formal conduction and report of an audit, auditing is generally necessary in order to be in full compliance. Entities falling under any of the privacy auditing regimes may wish to utilize immutable audit logs in order to ensure compliance.

II. FEDERAL AUDITING REQUIREMENTS FOR THE PRIVATE SECTOR

A. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

The Health Insurance Portability and Accountability Act ("HIPAA") was enacted to

> improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.[1]

Specifically, HIPAA's "Administrative Simplification" provisions authorized the Department of Health and Human Services ("HHS") to promulgate rules to ensure: (1) "[s]tandardization of electronic patient health, administrative and financial data;" (2) "[u]nique health identifiers for individuals, employers, health plans, and health care providers;" and (3) "[s]ecurity standards protecting the confidentiality and integrity of 'individually identifiable health information;' past, present or future."[2]

---

[1] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191,110 Stat. 1936, 1936 (1996), *available at* http://aspe.hhs.gov/admnsimp/pl104191.htm [hereinafter HIPAA].

[2] HIPAAdvisory, HIPAA Primer, http://www.hipaadvisory.com/regs/hipaaprimer.htm.

HIPAA is a broad and complex act that covers nearly all health care entities, including health care providers conducting certain electronic transactions, health care clearinghouses, and health plans.[3] As a federal auditing regime of private sector industry, its coverage is extensive. As of 2002, the health care sector comprised approximately 14% of the U.S. Gross Domestic Product.[4] HIPAA contains numerous provisions and severe civil and/or criminal penalties may be imposed for failure to comply with its requirements.[5] However, from the perspective of auditing for privacy of personal information the Administrative Simplification provisions are the most important. These provisions contain four main components: Standards for Electronic Transactions, Unique Identifiers Standards, the Security Rule, and the Privacy Rule.[6] Although HHS has promulgated numerous rules for each of these components, the Security Rule and the Privacy Rule are most relevant for the purposes of this article.

The Security Rule, which provides only for the protection of "electronic protected health information," is somewhat limited in its scope.[7] The rule became effective in April 2003. While most covered entities had to come into compliance with Security Rule standards by April 21, 2005, small health plans were given until April 21, 2006 to comply.[8] Generally, the Security Rule dictates that all covered entities must "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits."[9] The rule also requires covered entities to protect against any reasonably anticipated threats, uses, or disclosures that may undermine the security and integrity of such data

---

[3] HIPAA § 1171(3) (defining "health care provider"); *See also id.* HIPPA § 1171(2) (defining "health care clearinghouse"); *see also id.* at § 1171(5) (defining "health plan").

[4] ROSS C. DEVOL & ROB KOEPP, AMERICA'S HEALTH CARE ECONOMY 2 (2003), *available at* http://www.milkeninstitute.org/pdf/healthpole_fullreport_2003.pdf.

[5] HIPAAdvisory, *supra* note 2.

[6] *Id.*

[7] 45 C.F.R. § 164.302 (2005).

[8] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164).

[9] 45 C.F.R. § 164.306(a)(1).

or may be in conflict with the requirements of the Privacy Rule.[10] Additionally, covered entities are responsible for ensuring that all of their employees comply with these requirements.[11]

The HIPPA Security Rule is extremely general and vague. It provides health care entities with a great deal of flexibility and does not mandate any particular procedures or technologies. Specifically, the regulations state that "[c]overed entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart."[12] In order to make this determination, the entity must take many factors unique to its own business operations and systems into consideration, including complexity, capability, costs, and risks.[13]

As an additional example of generality and flexibility, the regulations also provide that only certain Security Rule standards are required, while others are merely "addressable."[14] Covered entities are only required to implement addressable specifications if those specifications are "reasonable and appropriate" when assessed in reference to the entity's particular environment.[15] If the entity chooses not to implement a particular addressable specification, it must document why the specification is not "reasonable and appropriate" and may implement an alternative that is more suitable.[16] Additionally, the entity is required to review these determinations and make modifications as necessary.[17] Therefore, an audit of the capabilities and risk potential of the entity's systems would be a useful tool in making decisions concerning addressable specifications. Although the regulations do not specifically state that an audit is required for this purpose, an audit would ensure that the entity is in

---

[10] *Id.*

[11] *Id.* § 164.306(a)(4).

[12] *Id.* § 164.306(b)(1).

[13] *Id.* § 164.306(b)(2).

[14] *Id.* § 164.306(d)(1).

[15] 45 C.F.R. § 164.306(d)(3)(ii)(A).

[16] *Id.* § 164.306(d)(3)(ii)(B).

[17] *Id.* § 164.306(e).

compliance. Additionally, if the entity had thoroughly tested, assessed, and documented such risks, it would have stronger proof of compliance in the case of a complaint.

On the other hand, the technical safeguard requirements of section 164.312 specifically state that audit controls are required under the Security Rule: "[i]mplement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."[18] This ties in closely with the integrity standard also required under Section 164.312 of the rule.[19] In order to ensure that its mechanisms to protect the integrity of electronic health information from alteration or destruction are effective, the covered entity must have some method of monitoring the data for changes. Although the technical safeguard requirements more specifically state the necessity of audits for HIPAA compliance, they are still extremely broad and flexible. There is little direction concerning the types of procedures that should be put in place, the necessary frequency of examinations, or the specific types of data, other than simply "electronic protected data," that should be examined and documented.

In addition to technical safeguards, the Security Rule also mandates administrative and physical safeguards.[20] Under the administrative safeguards, an "information system activity review" is required.[21] Specifically, the administrative safeguards of Section 164.308 require covered entities to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."[22] While this is the only portion of the administrative safeguards that specifically addresses the need for regular audits, full compliance with many other sections can not be achieved without audits. For example, the addressable specification, "access establishment and modification," provides that the covered entity should "implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a

---

[18] *Id.* § 164.312(b).

[19] *Id.* § 164.312(c)(1).

[20] *Id.* § 164.308.

[21] 45 C.F.R. § 164.308(a)(1)(ii)(D).

[22] *Id.*

workstation, transaction, program, or process."[23] If the business of a covered entity is of such a nature that this addressable specification is deemed critical, the entity may wish to conduct an audit of all user logins and responsibilities and make changes to access rights accordingly. In that case, if any issues arose concerning a breach of privacy by an unauthorized individual, the entity may be able to use this information to protect itself from liability. However, even as far as the administrative safeguards specifically require an audit, they, like the technical safeguards, do not provide covered entities with any clear, concise guidelines that must be followed.

The physical safeguards provision of the Security Rule is concerned with limiting physical access to information systems and does not contain any provisions that specifically address audits.[24] However, like the other two safeguard provisions, the examination and documentation of entry methods might be necessary for full compliance or to increase the probability of preventing liability. With that in mind, Section 164.316 states that covered entities must "implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements" of the Security Rule.[25] Even where audits are not specifically mandated by the Security Rule, it would be difficult to ensure the integrity of data or to protect data from unauthorized access. It is therefore important to have some mechanism in place to validate the data and determine if anyone has access to it that should not. Thus, it seems that in many organizations, an audit, even where not specifically required, would be an appropriate procedure for compliance with these standards. Additionally, under Section 164.314 of the Security Rule, the technical, administrative, and physical safeguards apply not only to the covered entity itself but also to its business associates through a contract or other agreement as mandated by Section 164.308(b).[26] Therefore, any business that has access to electronic protected health information through its relationship with a covered entity may also need audit controls in place to ensure compliance with Security Rule standards.

---

[23] *Id.* § 164.308(a)(4)(ii)(C).

[24] *Id.* § 164.310.

[25] *Id.* § 164.316(a).

[26] *Id.* § 164.314(a)(1); *See id.* §164.308(b).

The Privacy Rule is another key component of the HIPAA Administrative Simplification provisions. According to HHS, "the rule establishes the first 'set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care.'"[27] The Privacy Rule was published in December 28, 2000, but did not take effect until April 14, 2001. All covered entities were required to comply by April 14, 2003.[28]

The Privacy Rule gives patients rights to access their own medical records and restrict access to those records by others.[29] Patients may also see how their medical records have been accessed and request modifications to their records.[30] Most disclosures of protected health information ("PHI") can be restricted to the minimum amount of information needed for treatment and business operations.[31] However, patients may decide if they wish to allow access to their medical records for other reasons.[32] Additionally, all patients must receive formal notification of privacy practices.[33]

The Privacy Rule is broader in terms of its scope of coverage because while the Security Rule only covers electronic health information, the Privacy Rule covers data in both electronic and other forms.[34] However, in terms of auditing requirements the Privacy Rule is even more vague and general than the Security Rule. The Privacy Rule never specifically mentions audit controls. Rather Section 164.530 simply states that, "a covered entity must have in place

---

[27] HIPAAdvisory, *supra* note 2 (citing Standards for Privacy of Individually Identifiable Health Information; 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164)).

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] HIPAAdvisory, *supra* note 2.

[34] *Id.*

appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[35]

Thus, as under the Security Rule, covered entities are provided with a great deal of flexibility in determining how to meet the standards of the Privacy Rule. However, it would be difficult to ensure patient privacy without some form of audit. An audit may protect a covered entity from potential liability, and just like under the Security Rule, the stakes are high. The Privacy Rule imposes fairly severe criminal and civil sanctions for noncompliance. Additionally, the Privacy Rule, like the Security Rule, requires covered entities to form business associate agreements with their business partners. Therefore, the standards of this rule may be imposed on businesses other than traditional covered entities.[36]

B. THE GRAMM-LEACH-BLILEY ACT

The primary purpose of the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act ("GLB Act") is to protect the personal financial information of consumers that is held by financial institutions.[37] The GLB Act specifically applies only to personal information collected about individual consumers.[38] The Act does not cover information collected in the course of carrying out commercial activities.[39] The Act is comprised of three main components: the Financial Privacy Rule, the Safeguards Rule, and the pretexting provisions.[40]

The Financial Privacy Rule regulates both the collection and disclosure of personal customer information by financial institutions.[41] Additionally, the rule reaches other entities that receive such

---

[35] 45 C.F.R. § 164.530(c)(1).

[36] HIPAAdvisory, *supra* note 2.

[37] FTC Privacy Initiatives, The Gramm-Leach-Bliley Act, http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

[38] In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.pdf [hereinafter In Brief].

[39] *Id.*

[40] FTC Privacy Initiatives, *supra* note 37.

[41] *Id.*

information from financial institutions.[42] Specifically, the Act requires financial institutions to provide their customers with privacy notices that explain their privacy policy and practices for collecting and sharing information.[43] Customers are then able to place some limits on the sharing of their personal information.[44] The Financial Privacy Rule also restricts the ability of third-party financial institutions and other entities that receive personal information from a financial institution to utilize such information.[45]

The privacy notice required by the Safeguards Rule "must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information."[46] Additionally, it only applies to "nonpublic personal information." Any information that is believed to be "lawfully public" is not subject to the restrictions of the Act.[47] For the purpose of providing notice, the Financial Privacy Rule makes an important distinction between a *consumer* and a *customer*, with the extent of an institution's obligations being dependent upon this factor.[48] However, both *consumers* and *customers* have a right, with certain exceptions, to opt-out of having their information shared with others.[49]

---

[42] *Id.*

[43] In Brief, *supra* note 38.

[44] *Id.*

[45] FTC Privacy Initiatives, The Gramm-Leach-Bliley Act: The Financial Privacy Rule, http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html [hereinafter GLB: Financial Privacy Rule]; *see* 15 U.S.C. §§ 6801-6809 (2005).

[46] In Brief, *supra* note 38; *see* 15 U.S.C. S 6803 (2005); *see also* Press Release, Federal Trade Commission, Internet Service Provider Settles FTC Privacy Charges (Mar. 10, 2005), *available at* http://www.ftc.gov/opa/2005/03/cartmanager.htm (CartManager was found to be in violation of the Financial Privacy Rule after it rented out personal customer information collected from the customers of merchants doing business with the company to other marketers, knowing that this contradicted the merchants privacy policies as notified to their customers).

[47] In Brief, *supra* note 38; *see* 15 U.S.C. §§ 6801, 6809.

[48] In Brief, *supra* note 38.

[49] In Brief, *supra* note 38; *see* 15 U.S.C. §§ 6802(b), (e).

The Safeguards Rule is the most significant of the three rules in terms of auditing for privacy and security of customer financial information. This rule requires financial institutions, both those that receive personal information directly from their own customers and those that receive this information from other financial institutions, to "implement and maintain safeguards to protect customer information."[50] Specifically, the Safeguards Rule states that each agency given regulatory authority under the Act must establish standards for its jurisdiction,

> relating to administrative, technical, and physical safeguards -- (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[51]

The Safeguards Rule provides that the regulations will be enforced by either the federal functional regulators, state insurance authorities, or the Federal Trade Commission ("FTC") depending upon the type of institution in question. For example, brokers, dealers, and investment companies are subject to regulation by the Securities and Exchange Commission ("SEC");[52] insurance providers are regulated by applicable state insurance authorities,[53] credit unions are regulated by the Board of National Credit Union Administration ("NCUA");[54] and banks and savings associations are subject to regulation by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, or the Director of the Office of Thrift Supervision.[55] The FTC is responsible for all other institutions not

---

[50] FTC Privacy Initiatives, *supra* note 37.

[51] 15 U.S.C. § 6801(b).

[52] *Id.* § 6805(a)(1)(D)(3).

[53] *Id.* § 6805(a)(1)(D)(6).

[54] *Id.* § 6805(a)(1)(D)(2).

[55] *Id.* § 6805(a).

already covered.[56] Specifically, under the GLB Act, the FTC has jurisdiction over "non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors."[57] However, the FTC only has authority over entities that are "significantly engaged" in such financial activities.[58] Under the Safeguards Rule, these various agencies are required to coordinate with each other to ensure that the regulations promulgated by each are "consistent and comparable" across the board.[59] The rule also provides each agency with a deadline of six months from the enactment of the GLB Act to promulgate its regulations.[60] However, it does not appear that this goal was met.

The FTC published its final rule, entitled "Standards for Safeguarding Customer Information," in the Federal Register on May 23, 2002. The effective date for the FTC rule, covering all financial institutions under the FTC's jurisdiction, was May 23, 2003. However, existing service contracts were grandfathered until May 24, 2004.[61] The rule requires the development, implementation, and maintenance of an information security program that is "appropriate to your [the financial institution's] size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[62] An employee must be designated to coordinate the program. Additionally, in order to develop, implement, and maintain the program, financial institutions have the following obligations:

> [i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such

---

[56] *Id.* § 6805(a).

[57] In Brief, *supra* note 38.

[58] *Id.*

[59] 15 U.S.C. § 6804(a)(2).

[60] *Id.* § 6804(a)(3).

[61] 16 C.F.R. § 314.5(b).

[62] *Id.* § 314.3(a).

> information, and assess the sufficiency of any safeguards in place to control these risks.[63]

In this assessment, the covered entity must analyze the risks involved in numerous operational areas, including management and employee training, design, processing, storage, and disposal of information systems, and processes to prevent, detect, and respond to security breaches.[64] Financial institutions must use the results of this analysis to implement safeguards that must be tested regularly. The results of those tests must be used to "evaluate and adjust your [the] information security program."[65] Financial institutions must also review their service providers to ensure they are capable of providing the necessary safeguards.[66] Therefore, they should contract with service providers to create and maintain such safeguards.[67]

Neither the GLB or the FTC rule provide any specific requirements concerning the type and amount of information that must be reviewed, the procedures that must be followed for audit, or the frequency in which such reviews must take place. However, it is obvious from the language of the FTC rule that a thorough audit of information security practices is required in order for full compliance. An audit may help to guard a financial institution from liability in the face of a customer complaint or an FTC review for compliance. In cases where the FTC has found a financial institution in violation of the Safeguards Rule, it has enforced the requirement of biannual audits for a term of up to ten or even twenty years from the date of the violations.[68]

The SEC's final rule contains even less extensive information than the FTC's. It does little more than reiterate the three objectives that

---

[63] *Id.* § 314.4(b).

[64] *Id.*

[65] *Id.* § 314.4(e).

[66] *Id.* § 314.4(d)(1).

[67] *Id.* § 314.4(d)(2).

[68] *See generally* Press Release, Federal Trade Commission, BJ's Wholesale Club Settles FTC Charges (Jun. 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.htm; *see also* Press Release, Federal Trade Commission, DSW Inc. Settles FTC Charges (Dec. 1, 2005), *available at* http://www.ftc.gov/opa/2005/12/dsw.htm; *see also* Press Release, Federal Trade Commission, FTC Enforces Gramm-Leach-Bliley Act's Safeguards Rule Against Mortgage Companies (Nov. 16, 2004), *available at* http://www.ftc.gov/opa/2004/11/ns.htm.

are listed in the GLB Act and does not provide any additional direction for meeting these objectives.[69] Although the guidelines issued by the NCUA are slightly more comprehensive overall, requiring a number of mechanisms for managing and controlling risk, such as board involvement, encryption, segregation of duties, dual control procedures, and monitoring systems, the guidance provided on auditing processes to asses these risks is limited. Similar to the FTC rule, the NCUA guidelines simply state that the information security program should be tested and adjusted as needed, and service providers should be carefully selected and monitored as necessary.[70] However, one significant difference is that the NCUA contains an annual reporting requirement. As stated in the NCUA guidelines,

> [e]ach credit union should report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the credit union's compliance with these guidelines. The report should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.[71]

The remaining agencies, the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision issued joint guidelines that also require a reporting requirement and contain identical language to that of the NCUA guidelines.[72]

The pretexting provisions are intended to prohibit individuals and organizations from obtaining consumer information from financial

---

[69] 17 C.F.R. §§ 248.30(a)(1)-(3) (2005).

[70] Guidelines for Safeguarding Member Information, 12 C.F.R. § 748, app. A (III)(F) (2005).

[71] 12 C.F.R. § 748, app. A (III)(F) (2005).

[72] Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616, 8,620-25 (Feb. 1, 2001) (to be codified at 12 C.F.R. pts. 30, 208, 211, 225, 263, 308, 364, 568, 570).

institutions under false pretenses.[73] These provisions make it unlawful to even attempt to obtain such consumer information through the use of fraudulent documentation, or statements, or misrepresentation.[74] However, several exceptions are provided for law enforcement agencies, insurance institutions, and even financial institutions in certain cases.[75] Interestingly, the exception for financial institutions is allowed for auditing purposes. Specifically, the pretexting provisions do not prevent financial institutions from obtaining customer information for the purpose of: "testing the security procedures or systems of such institution for maintaining the confidentiality of customer information; or investigating allegations of misconduct or negligence on the part of any officer, employee, or agent of the financial institution."[76]

C. SARBANES-OXLEY

The Sarbanes-Oxley Act of 2002 was the result of a number of financial scandals in large public corporations such as Enron and WorldCom.[77] The Act requires a number of companies to submit a report annually to the SEC on the "effectiveness" of their internal accounting controls.[78] Companies are required to come into full compliance between November 2006 and July 2006 depending on their size. By July 2006, all companies covered by the Act must comply on a quarterly basis.[79] The Act covers all public companies doing business in the United States including foreign corporations. It also covers wholly owned subsidiaries and may affect private

---

[73] In Brief, *supra* note 38; *see* 15 U.S.C. §§ 6821-6827 (2005).

[74] 15 U.S.C. § 6821(a).

[75] *Id.* §§ 6821(c)-(e).

[76] *Id.* §§ 6821(d)(1)-(2).

[77] Sarbanes-Oxley-101.com, Need a Sarbanes Oxley Compliance Plan?, http://www.sarbanes-oxley-101.com/sarbanes-oxley-faq.htm (last visited Feb. 26, 2006); *see generally The Fall of Enron,* CHRON.COM, http://www.chron.com/news/specials/enron/ (last visited Feb. 26, 2006); *see also* WorldCom Fraud InfoCenter, http://www.worldcomfraudinfocenter.com/ (last visited Feb. 26, 2006).

[78] Sarbanes-Oxley-101.com, *supra* note 77.

[79] *Id.*

companies preparing for an IPO.[80] This is the only sense in which Sarbanes-Oxley takes the size and nature of companies into account. The Act is not scalable in the same sense as HIPAA, meaning that the standards do not vary across companies depending on the potential risk for each specific company. Once a company meets the qualifying criteria above, the same auditing requirements will be imposed on all companies.[81] Every public company must have an audit committee composed wholly of independent directors. The NYSE and NASDAQ are directed to prohibit listing to any public company that fails to comply.[82]

Unlike HIPAA and the GLB Act, Sarbanes-Oxley is not a privacy auditing act. It does not focus on personal customer or patient information; rather, it targets the financial data of the company.[83] Sarbanes-Oxley requires an increase in the disclosure of all financial statements. For example, of the eleven sections comprising the Sarbanes-Oxley Act, Section 409 requires companies to disclose, on an "almost real-time basis[,] information concerning material changes in its financial condition or operations."[84]

However, some particular requirements of Sarbanes-Oxley may cross over into personal information. For example, Section 404 requires management to review the effectiveness of internal controls.[85] Any "shortcomings" must be reported and external auditors must verify the accuracy of management's assessment. This includes documenting all revisions to financial data – who made a change, when he or she made it and why.[86] An additional distinguishing factor between HIPAA, GLB, and Sarbanes-Oxley is that Sarbanes-Oxley specifically requires an audit that must be documented, verified by

---

[80] *Id.*

[81] *Id.*

[82] Sarbanes-Oxley Act of 2002, http://www.cpeonline.com/cpenew/sarox.asp (last visited Aug. 21, 2006).

[83] Sarbanes-Oxley-101.com, *supra* note 77.

[84] Sarbanes-Oxley-101.com, Sarbanes Oxley Compliance, http://www.sarbanes-oxley-101.com/SOX-409.htm (last visited on Aug. 21, 2006).

[85] Sarbanes-Oxley-101.com, Info Guide to Sarbanes Oxley Act of 2002, http://www.sarbanes-oxley-101.com/SOX-404.htm (last visited on Aug. 21, 2006).

[86] *Id.*

external auditors, and submitted to the SEC, while under HIPAA and GLB audits are only used internally unless compliance problems arise.[87] Additionally, the requirements for Sarbanes-Oxley are very specific. Companies must closely follow requirements concerning the types of information to be reported and the mechanisms for reporting that information.[88]

III. FEDERAL AUDITING REQUIREMENTS FOR PUBLIC SECTOR

A. GOVERNMENT INFORMATION SECURITY REFORM ACT/FEDERAL INFORMATION SECURITY MANAGEMENT ACT

The Government Information Security Reform Act ("GISRA") was included in The Defense Authorization Act (Public Law 106-398), which became effective on November 29, 2001 and was to sunset in two years.[89] Covering both unclassified and national security systems, the Act "seeks to ensure proper management and security for the information resources supporting Federal operations and assets."[90] GISRA specifically requires federal agencies to complete an audit of agency-wide information systems through an "annual program review." Although the Act itself does not provide a great deal of detail on the requirements of this review, it authorizes the Chief Information Officers ("CIO") Council's Federal Information Technology Security Framework to form basic standards in the interest of promoting consistency across the government.[91] Each agency must then report the results of its review, including an independent evaluation, to the Office of Management and Budget ("OMB") as part of its yearly budget submission.[92]

---

[87] *See id.*

[88] *See id.*

[89] Memorandum from Jack Lew, Director, Office of Management and Budget, to the Heads of Executive Departments and Agencies 1 (Jan. 16, 2001), *available at* http://www.whitehouse.gov/omb/memoranda/m01-08.pdf.

[90] *Id.*

[91] *Id.* at 7.

[92] *Id.*

Prior to the sunset of GISRA, the Federal Information Security Management Act ("FISMA") was proposed as part of the 2002 e-government bill (public law 107-347) to "permanently reauthorize" GISRA.[93] Like HIPAA, FISMA is scalable to the extent that federal agencies are required to provide "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of" agency information systems or information contained therein.[94] However, the requirements of FISMA are much more formal than those of HIPAA because they go further than stating that audit controls must be in place. Specifically, the statute requires "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually."[95] This specific requirement of auditing frequency is more in line with Sarbanes-Oxley.

Also like Sarbanes-Oxley, FISMA requires an annual report to the government, whereas under HIPAA and GLB,audit results may never be reported externally unless there are complaints or suspicions of noncompliance. According to FISMA, each agency must

> report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter.[96]

Additionally, FISMA, like Sarbanes-Oxley, is more robust than HIPAA in that it provides agencies with more specific standards to

---

[93] *WashingtonTechnology.com,GISRA Update*, WASH. TECH., July 15, 2002, http://www.washingtontechnology.com/news/17_8/datastream/18557-1.html.

[94] 44 U.S.C. § 3544(a)(1)(A) (2005).

[95] *Id.* § 3544(b)(5).

[96] *Id.* § 3544(c)(1).

follow in the performance of audits. The National Institute of Standards and Technology ("NIST") is currently working on finalizing these standards to promote consistency in controls across government agencies.[97] NIST is responsible for providing guidance through Federal Information Processing Standards and an 800 series of Special Publications.[98]

B. CHIEF PRIVACY OFFICER REQUIREMENT

A bill passed on December of 2004 known as the Strengthening Homeland Innovation by Emphasizing Liberty, Democracy, and Privacy Act, or Shield Privacy Act, which requires all federal agencies of all sizes and functions to designate a Chief Privacy Officer. These privacy officers will be responsible for ensuring that the databases maintained by federal agencies are in compliance with the Code of Fair Information Practices.[99] All federal agencies must hire an external auditor to complete an audit of the agency twice a year in order to ensure compliance with federal privacy laws.[100]

Additionally, under the Shield Privacy Act, the Office of Management and the Budget is responsible for designating a high level Chief Privacy Officer, or privacy czar, that will oversee the privacy policy of all the federal agencies. Prior to the passage of the Shield Privacy Act, the Department of Homeland Security was the only agency that was required to have a Chief Privacy Officer.[101] However, the IRS had designated a Chief Privacy Officer as well. The privacy officers will be responsible for ensuring that the databases maintained by federal agencies are in compliance with the Code of Fair Information Practices.[102]

---

[97] NIST, FISMA Implementation Project, Security Categorization, http://csrc.nist.gov/sec-cert/ca-categorization.html (last visited Feb. 26, 2006).

[98] William Jackson, *FISMA Guidance Nearly Complete*, GOV'T COMPUTER NEWS, Oct. 26, 2005, http://www.gcn.com/vol1_no1/FISMA/37422-1.html?topic=FISMA.

[99] Ryan Singel, *What Price Privacy?*, WIRED NEWS, Dec. 9, 2004, http://www.wired.com/news/politics/0,1283,65973,00.html?tw=wn_story_related.

[100] *Id.*

[101] The Homeland Security Act, 6 U.S.C. § 142 (2005).

[102] Singel, *supra* note 99.

Many have criticized the Act for being too broad to adequately meet the needs of different agencies. Unlike HIPAA and GLB, which have scalable requirements, the Shield Privacy Act is more similar to Sarbanes-Oxley in that all agencies must meet the same requirements regardless of size or function. According to Peter Swire, President Clinton's Chief Counselor for Privacy, "[s]ome agencies face major privacy issues, including the Department of Health and Human Services and the Justice Department . . . . Others really only have privacy issues for their own employees. The level of auditing and scrutiny should be much greater for the key agencies."[103] Other critics argue that the Shield Privacy Act undermines the authority of the Chief Information Officer ("CIO"). Although the OMB seems to oppose the provision, it has issued a memo directing agencies to appoint a senior agency official.[104] However, the memo seems to contradict the Act and does not require the designation of a "chief" of privacy. It also implies that the CIO may serve the role. Although the bill has many supporters as well, a bill repealing the provision was introduced just shortly after its passage.[105]

C. GAO AUDITS

In addition to agency oversight by a chief privacy officer, the Government Accountability Office ("GAO") also performs audits of federal agencies.[106] The GAO is authorized by Congress to conduct reviews of federal government programs and expenditures. It is an independent, non-partisan organization that is frequently referred to as the "investigative arm of Congress" or the "Congressional Watchdog."[107] The GAO works with Congress and federal agency leaders to improve the effectiveness and responsiveness of government. It also issues legal opinions, reports the results of its studies to Congress, and recommends actions for improvements.[108]

---

[103] *Id.*

[104] David Perera, *The Need for Privacy – Should every Agency have a Chief Privacy Officer?*, FCW.COM, Apr. 11, 2005, http://www.fcw.com/article88549.

[105] *Id.*

[106] GAO, What is GAO?, http://www.gao.gov/about/what.html (last visited Feb. 13, 2006).

[107] *Id.*

[108] *Id.*

The GAO has conducted numerous audits concerning privacy initiatives to ensure that agencies are meeting legal requirements and calling for corrective actions when they are not. Recently, in July of 2005, the GAO performed an audit of the Transportation Security Administration's ("TSA") Secure Flight Program.[109] As part of this audit the GAO reviewed the TSA's compliance with the Privacy Act. According to the GAO, the results of this study showed that the TSA failed to comply with the Privacy Act because it did not make full disclosure to the public concerning its use of personal information.[110] Particularly, the TSA drew information from commercial sources in order to test its secure flight program without informing the public.[111] Although the TSA did issue privacy notices in the Federal Registrar prior to the testing, it failed to fully inform the public concerning the scope of information used or its own or its contractors' procedures for collecting, storing, and using this data.[112] The GAO reported the results of the secure flight audit to Congress, and in response to its comments, the TSA issued revised privacy notices in the Federal Registrar.[113]

The GAO performs routine audits of many federal agency programs including the Privacy of Consumer Information Rule promulgated by the SEC as part of the GLB Act.[114] In this study, the GAO performed a cost-benefit analysis of the Act and ensured compliance with other federal laws. The report was positive.[115] The GAO also made a positive report indicating compliance with all applicable requirements on the Department of Health and Human

---

[109] Posting of Bruce Schneier to Schneir on Security, http://www.schneier.com/blog/archives/2005/07/secure_flight.html (July 24, 2005).

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] Todd R. Weiss, *GAO: Secure Flight Antiterror Program Violates Privacy Laws*, COMPUTERWORLD, July 26, 2005, http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,103482,00.htm.

[114] Securities and Exchange Commission: Privacy of Consumer Financial Information (Regulation S-P), July 12, 2000, http://www.gao.gov/archive/2000/og00041.pdf.

[115] *Id.*

Services implementation of HIPPA.[116] For a full list of GAO reports, visit the official site for GAO reports at http://www.gao.gov/docsearch/repandtest.html.

IV. USING IMMUTABLE AUDIT LOGS TO INCREASE SECURITY AND COMPLY WITH PRIVACY AUDITING REGIMES

As previously mentioned, the HIPAA Security Rule specifically requires logging. Although many of the privacy auditing regimes discussed in this paper do not state such a requirement explicitly, the practice may be helpful for assuring compliance and possibly refuting liability. The Markle Foundation has suggested the use of immutable audit logs ("IALs") to log system activity in information sharing systems in order to ensure and demonstrate compliance with policies and laws.[117] This can be particularly useful to provide oversight and increase confidence in classified systems. Major technical and policy concerns with IALs include decisions on what to log and how long to store the information.[118] Immutable logs provide advantages over ordinary mutable logs because they are not as susceptible to unauthorized modifications.[119] However, there may still be issues of tampering in original transactions. Additionally, IALs themselves may be at risk for misuse and disclosure. Thus, restrictions on their use and other precautions should be taken to prevent unauthorized access.[120] "Any audit—whether based on mutable or immutable logs—provides benefits, including the ability to deter, detect, and prove policy

---

[116] Government Accounting Office (GAO), Analysis of the DHHS Rule Entitled "Standards for Privacy of Individually Identifiable Health Information," Aug. 22, 2002, http://www.gao.gov/decisions/majrule/d021046r.pdf.

[117] The Markle Foundation Task Force on National Security in the Information Age, Implementing a Trusted Information Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability (Feb. 2006), *available at* http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf.

[118] *Id.* at 3.

[119] *Id.* at 1-3.

[120] *Id.* at 4-6.

violations."[121] However, there are barriers to implementing IALs such as costs, performance effects on other systems, and privacy.[122]

V. CONCLUSION

Over the past decade, congress has created a number of privacy auditing regimes in an attempt to increase the privacy of both individual consumers and the federal government. With the exception of Sarbanes-Oxley, which is not even a true privacy auditing regime, the private sector regimes seem to be lacking in robustness, scalability, and specificity. Unlike the public sector regimes, the private sector regimes provide covered entities with very little direction and generally do not require these entities to submit formal reports. The Sarbanes-Oxley Act, an outlier as far as private sector privacy auditing regimes are concerned, more closely matches the regimes for federal government oversight than the other private sector regimes. However, this does not mean that entities covered under HIPAA and GLB do not have to be concerned about consumer privacy. Although the private sector privacy acts do not explicitly require auditing, auditing seems to be a necessity for compliance. These entities may not be required by law to submit a quarterly or annual report, but an investigation may be conducted at any time, and it may be difficult to pass such investigations without audit reports. Furthermore, covered entities may face severe civil and/or even criminal penalties for noncompliance. Therefore, all covered entities, including those in the private sector, should consider auditing for privacy and may also want to consider the use of IALs as a tool to ensure compliance.

---

[121] *Id.* at 1.

[122] *Id.* at 4-6.